UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/812,622	03/30/2004	Kazumasa Omote	1924.70199	3471

7590 06/15/2009

Patrick G. Burns, Esq.
GREER, BURNS & CRAIN, LTD.
Suite 2500
300 South Wacker Dr.
Chicago, IL 60606

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/812,622	OMOTE ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,8,13,15-18,22-25,27,28,34,35,41 and 43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,8,13,15-18,22-25,27,28,34,35,41,43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3-9-2009 2-18-2009 1-6-2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Applicant's submission filed on 3-30-2009 has been entered.

2. Claims **1, 3 - 5, 8, 13, 15 - 19, 22 - 25, 27, 28, 34, 35, 41, 43** are pending. Claims **1, 3, 5, 8, 13, 15, 16, 18, 22 - 25, 27, 28** have been amended. Claims **2, 6, 7, 9 - 12, 14, 19 - 21, 26, 29 - 33, 36 - 40, 42** have been cancelled. Claims **1, 3, 5, 8, 13, 15, 16, 18, 22, 23, 24, 25, 27, 28, 34, 35** are independent. This application was filed on 3-20-2004.

Response to Arguments

3. Applicant's arguments have been fully considered but were not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose *"unit time of measurement". (see Remarks Page 25, 26, 28, 33, 36)*

Spiegel prior art discloses monitoring network traffic such as network packets and analyzing the monitored traffic to determine whether the communications is from a network node infected by a worm. The analysis is completed over a period of time.

(see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic; col. 3, lines 20-24: connection attempts to remote destinations over a period of time)

3.2 Applicant argues that the referenced prior art does not disclose *"changing setting information". (see Remarks Page 25, 33, 36); "changing judgment criteria". (see Remarks Page 27, 38)*

Spiegel prior art discloses that parameters are adjustable or changeable and can be changed or weighted based on other parameters. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable) parameters for worm determination; relative (percentage) parameters used; col. 5, lines 47-53: heuristic can be fine tuned)

Willebeek-LeMair prior art discloses self-hardening of the detection system which optimizes the capabilities of the monitoring system. (Willebeek-LeMair paragraph [0054], lines 1-14: tuning operation performed in an automated manner; paragraph [0055], lines 1-17: effectuates a self-hardening system; paragraph [0056], lines 1-16: threat detection and threat suppression (firewall) capabilities of the system are continually being optimized (by the interlocking and agent functionalities in response to continuous threat assessment analysis))

3.3 Applicant argues that the referenced prior art does not disclose *"judging that a plurality of computer are infected by a worm". (see Remarks Page 29, 40)*

Siegel prior art discloses a determination that communication is executed by a

system infected by a worm. Spiegel prior art and its combination with Willebeek-LeMair and Bunker disclose the criteria of a large number of packets and additional criteria used to make the determination of communication from a system infected by a worm. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses and information not matching criteria for normal traffic setting; col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

3.4 Applicant argues that the referenced prior art does not disclose *"comparing features of communication judged to be a worm". (see Remarks Page 31)*

Spiegel prior art discloses that previously recorded information or historical information can be analyzed and compared to current communication information in order to make a determination of whether communication is coming from an infected worm. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination) In addition, threshold limitations in data processing disclose a comparison of a current parameter value against a threshold value to determine a course of action.

3.5 Applicant argues that the referenced prior art does not disclose *"summing number of packets for each port". (see Remarks Page 42, 43, 45-48)*

Spiegel prior art discloses the usage of threshold criteria to make a determination of communication from a system infected by a worm. A threshold is maximum limit parameter. A current count of communication packets for connection attempts must be

counted or summed and the current count of these types of packets are compared against a limit or threshold parameter.

Willebeek-LeMair prior art discloses the specific extraction of reference information such as a port number from a communications packet. Willebeek-LeMain prior art discloses the usage of port number information in the analysis of communication traffic. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

3.6 Spiegel prior art discloses the monitoring of network traffic from events such as connection attempts which are performed using network communication packets. Analysis of connections attempts are used in the determination of a system being infected by a worm. Spiegel prior art discloses the usage of historical information in the analysis of communications to determination of input from a system infected by a worm.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1, 3 - 5, 8, 13, 15 - 18, 22 - 24, 34, 41, 43** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel et al.** (US Patent No. **7,159,149**) in view of **Willebeek-LeMair et al.** (US PGPUB No. **20030204632**).

With Regards to Claims 1, 13, 15, Spiegel discloses a computer readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

a) acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement. (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic setting; col. 3, lines 20-24: connection attempts to remote destinations over a period of time; col. 2, lines 51-53; col. 2, lines 62-65; col. 6, lines 15-22: software, implementation means)

Furthermore, Spiegel discloses:

b) judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; (see Spiegel col. 1, lines 60-67; col. 3, line 63 - col. 4, line 9: determine communications due to worm, based on threshold or predetermined criteria)

e) changing the setting information upon it being judged at the judging that the communication is executed by the worm; wherein the acquiring includes acquiring the information based on the setting information changed at the changing. (see Spiegel col. 5, lines 15-21: dynamic (i.e. adjustable, changeable)

parameters used for worm determination; col. 5, lines 47-53: heuristic can be fine tuned; col. 6, lines 15-26: software, implementation means)

Spiegel does not specifically disclose extracting specific information and blocking communication packet.

However, Willebeek-LeMair discloses:

c) extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

d) blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting. (see Willebeek-LeMair paragraph [0017], lines 12-15; paragraph [0031], lines 5-14; paragraph [0035], lines 7-14: block communications packets between network segments (inside network segment and outside network segment))

It would have been obvious to one of ordinary skill in the art to modify Spiegel for extracting specific information and blocking communication packet as taught by Willebeek-LeMair. One of ordinary skill in the art would have been motivated to employ the teachings of Willebeek-LeMair for threat detection and threat response operational in an optimized manner that mitigates false detection. (see Willebeek-LeMair paragraph [0013], lines 5-11)

With Regards to Claims 3, 16, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; as stated in Claim 1 above.

Furthermore, Spiegel discloses for following:

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

changing the judgment criteria upon it being judged at the judging that the communication is executed by the worm, wherein the judging includes further judging whether the communication is executed by the worm based on the information acquired and the judgment criteria changed at the changing. (see Spiegel col. 5, lines 8-10; col. 5, lines 15-21: worm determination based on information and adjusted (i.e. changed) information; col. 6, lines 15-22: software, implementation means)

Spiegel does not specifically disclose extracting information and blocking communication.

However, Willebeek-LeMair discloses the following:

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; as stated in Claim 1 above;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claims 4, 17, Spiegel discloses the computer readable recording medium, device according to claims 1, 15, the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 3, lines 20-27: network communication packets throughput increased, worm determination; col. 4, lines 17-22: number of destination addresses is high; col. 6, lines 15-22: software, implementation means)

With Regards to Claims 5, 18, Spiegel discloses a computer-readable recording

medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; as stated in Claim 1 above.

Furthermore, Spiegel discloses the following:

first judging whether a computer in the predetermined network segment is infected by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

second judging whether a plurality of computers in the predetermined network segment are infected by the worm; (see Spiegel col. 1, lines 50-60; col. 3, lines 27-30: monitor network traffic based on source and destination addresses, and information not matching criteria for normal traffic setting; col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored)

the second judging includes judging that plurality of computers in the predetermined network segment are infected by the worm; (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored)

f) a communication from the computer in the predetermined network segment is

judged to be infected by the worm at the first judging; (see Spiegel col. 5, lines 8-10: history of worm detection; col. 5, lines 47-50: particular source/destination addresses (i.e. for a computer) monitored; col. 6, lines 15-22: software, implementation means)

g) a number of destination addresses of the communication packets that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging. (see Spiegel col. 3, lines 20-27: worm determination based on number of packets transferred to addresses (i.e. inside or outside local network); connection attempts (destination addresses))

Spiegel does not specifically disclose extracting information and blocking communication.

However, Willebeek-LeMair discloses the following:

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the first judging that the computer is infected by the worm; as stated in Claim 1 above;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 8, Spiegel discloses a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; as stated in Claim 1 above.

Furthermore, Spiegel discloses the following:

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above;

the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that are recorded in advance. (see Spiegel col. 3, lines 58-67: worm determination; col. 5, lines 8-15: history or recorded information utilized in worm determination; col. 6, lines 15-22: software, implementation means)

Spiegel does not specifically disclose extracting information and blocking

communication.

However, Willebeek-LeMair discloses the following:

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; as stated in Claim 1 above;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claims 22, 23, 24, 34, Spiegel discloses a computer-readable recording medium for storing a computer program, device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; as stated in Claim 1 above.

Furthermore, Spiegel discloses:

judging whether the communication is executed by the worm based on the

information acquired and a predetermined judgment criteria; as stated in Claim 1 above.

Spiegel does not specifically disclose extracting port information and blocking communication.

However, Willebeek-LeMair discloses the following:

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; as stated in Claim 1 above;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above;

the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication. (see Willebeek-LeMair paragraph [0031], lines 5-14: extract reference information (IP address, port number))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 41, Spiegel discloses the computer-readable recording medium according to claim 3, the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based

on communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm)

Spiegel does not specifically disclose an increase in number of communication packets that are transmitted.

However, Willebeek-LeMair discloses an increase in number of communication packets that are transmitted. (Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

With Regards to Claim 43, Spiegel discloses the computer-readable recording medium according to claim 8, the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm based on communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside. (see Spiegel col. 1, lines 50-62: connections attempts (communication packets) directed to a destination address used in determination of a worm)

Spiegel does not specifically disclose an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted.

However, Willebeek-LeMair discloses an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted. (Willebeek-LeMair paragraph [0007], lines 8-12: large numbers of packets and connection requests (destination address))

Motivation to modify Spiegel as taught by Willebeek-LeMair is stated in Claim 1 above.

6. Claims **25, 27, 28, 35** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Spiegel-"Willebeek-LeMair"** and further in view of **Bunker et al.** (US PGPUB No. **20030056116**).

With Regards to Claims 25, 27, 28, 35, Spiegel discloses the computer program, computer-readable medium, method, and device according to claims 1, 12, 13, 14, 33. (see Spiegel col. 1, lines 48-62: monitoring for worm determination; col. 4, lines 45-48: traffic analysis, calculation utilizing network addressing (IP address, port number)) a computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information including unit time for measurement; as stated in Claim 1 above.

Furthermore, Spiegel discloses:

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment criteria; as stated in Claim 1 above.

Spiegel does not specifically disclose extracting information such as a port number and blocking communication.

However, Willebeek-LeMair discloses the following:

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; as stated in Claim 1 above;

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting; as stated in Claim 1 above.

Spiegel does not specifically disclose calculations utilizing reference information such as port numbers in the analysis of work determination.

However, Bunker discloses extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication, the number of the communication packets is over a threshold value. (see Bunker paragraph [0189], lines 1-11; paragraph [0215], lines 1-5; paragraph

[0220], lines 8-12: calculation (summation) of access information in worm determination)

It would have been obvious to one of ordinary skill in the art to modify Spiegel to calculate a summation of reference information utilized for worm determination as taught by Bunker. One of ordinary skill in the art would have been motivated to employ the teachings of Bunker to emulate hacker methodology in a safe way and enable study of network security openings without affecting customer operations. (see Bunker paragraph [0012], lines 1-8)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
May 26, 2009